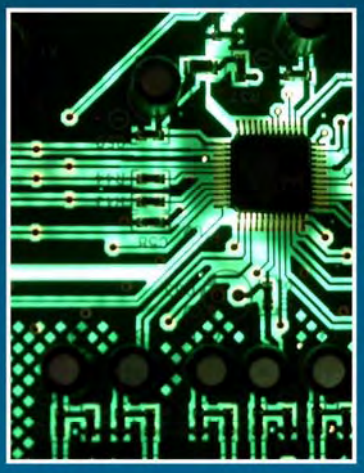
ANNUAL REPORT
TO CONGRESS ON



FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE

2007

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
10 SEP 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Annual Report to Congress: Foreign Economic Collection and Industrial Espionage 2007	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the National Counterintelligence Executive,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**22**	

10 September 2008

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY07

This assessment was prepared by the Office of the National Counterintelligence Executive. Comments and queries are welcome and may be directed to the Chief, Analysis and Collection, ONCIX, on (571) 204-5063 or 25174 secure.

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY07

Key Findings

The United States remains the prime target for foreign economic collection and industrial espionage by virtue of its global technological leadership and innovation. Collectors from across the globe—private businessmen, scientists, engineers, students, and foreign military and intelligence officers—engaged in economic collection activities against the United States in Fiscal Year 2007 (FY 2007), according to information amassed by the Counterintelligence (CI) Community. While collectors came from a large number of countries, those from fewer than 10 nations, including both allies and adversaries, accounted for the bulk of targeting activity.

Foreign collectors continue to target a wide variety of unclassified and classified information and technologies in a range of sectors. According to the CI Community, which has the most detailed information on foreign collection efforts against dual-use, export-controlled, and military items, the most heavily targeted sectors across all agencies include aeronautics, information technologies, lasers, sensors, optics, and armaments and energetic materials. Targets also include the unique manufacturing processes and trade secrets used to produce technological goods and services.

The methods employed by collectors remain as diverse as the collectors themselves. They include direct requests, solicitation and marketing of services, acquisition of technologies and companies, targeting at conferences or other open venues, exploitation of joint research and official visits, and targeting of US travelers overseas. Collectors increasingly make use of technologically sophisticated methodologies such as cyber attack and exploitation, which obfuscate their identities and goals.

Tracking, analyzing, and countering foreign collection efforts are increasingly difficult challenges as the growth of multinational organizations in the increasingly global marketplace compounds and obscures the threat to the United States.

Scope Note

This annual assessment is submitted in compliance with the Intelligence Authorization Act for Fiscal Year 1995, Section 809(b), Public Law 103-359, which requires that the President annually submit to Congress updated information on the threat to US industry from foreign economic collection and industrial espionage. This report updates the *12th Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2006* and includes data from fiscal year 2007.

The report reviews the threat to US industry by foreign economic collection and industrial espionage and identifies trends such as the number and identity of foreign governments conducting industrial espionage, the industrial sectors and types of information and technology targeted by such espionage, and the methods used to conduct such espionage.

As in previous years, this report covers a range of activities that fall under the rubric of "industrial espionage," which are directed at trade secrets. In this context, "trade secrets" includes the following: all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether stored or unstored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if the owner (i.e., the person or entity in whom or in which rightful legal or equitable title to, or license in, is reposed) has taken reasonable measures to keep such information secret and the information derives independent economic value, actual, or potential from not being generally known to, and not being readily ascertainable through, proper means by the public. Activities to improperly acquire trade secrets include:

- **Economic Espionage**, which is the conscious and willful misappropriation of trade secrets with the knowledge or intent that the offense will benefit a foreign government, foreign instrumentality, or foreign agent. Misappropriation includes, but is not limited to, the following activities: stealing, copying, altering, destroying, transmitting, sending, receiving, buying, possessing, or conspiring to misappropriate trade secrets without authorization. Section 101(a) of the Economic Espionage Act of 1996 (EEA) criminalizes economic espionage.

- **Industrial Espionage**, which is the conscious and willful misappropriation of trade secrets related to, or included in, a product that is produced for, or placed in, interstate or foreign commerce to the economic benefit of anyone other than the owner, with the knowledge or intent that the offense will injure the owner of that trade secret. Misappropriation includes, but is not limited to, the following activities: stealing, copying, altering, destroying, transmitting, sending, receiving, buying, possessing, or conspiring to misappropriate trade secrets without authorization. Industrial espionage is also criminalized under the EEA.

- **Export Control Violations.**

Transfer of dual-use equipment and technology, which includes unauthorized acquisition of restricted US dual-use items (having both military and civil applications) by countries or persons that might apply such items in ways that are inimical to US interests. These items include goods and technologies that might be related to the proliferation of weapons of mass destruction and their delivery and those that could bolster the military capability and terrorist activity of certain countries. The Department of Commerce's (DOC) Bureau of Industry and Security is responsible for the regulation of exports for national security, foreign policy, and nonproliferation reasons and the enforcement of those regulations. The Federal Bureau of Investigation (FBI) and US Immigration and Customs Enforcement (ICE) maintain concurrent jurisdiction to enforce violations of these rules. According to the Code of Federal Regulations (28 CFR § 0.85(d)), the FBI is to take charge of the counterintelligence (CI) aspects of export cases. These organizations coordinate their investigative efforts to ensure that all prosecutorial options are maintained.

Transfer of defense items, which includes unauthorized export of defense articles, defense services, and related technical data (collectively known as the US Munitions List). Munitions List items include arms and implements of war. The State Department's Directorate of Defense Trade Controls administers the International Traffic in Arms Regulations (ITAR), and ICE enforces violations of the Arms Export Control Act and ITAR. The State Department maintains a policy of denying exports of items on the Munitions List to proscribed countries.

In 2007, the Department of Justice appointed the first National Export Control Coordinator to improve the investigation and prosecution of illegal exports of US arms and sensitive technology. Full coordination between the Department of Justice and the various US law enforcement, licensing,

and intelligence agencies that play a role in export enforcement will be critical to future successful prosecutions.

The Office of the National Counterintelligence Executive compiled this report on the basis of inputs from a broad spectrum of US Government agencies and departments, including:

- Air Force Office of Special Investigations.
- Army Counterintelligence Center.
- Central Intelligence Agency.
- Defense Intelligence Agency.
- Defense Security Service.
- Department of Commerce, Bureau of Industry and Security.
- Department of Energy.
- Department of Homeland Security, US Immigration and Customs Enforcement.
- Department of State.
- Federal Bureau of Investigation.
- National Geospatial-Intelligence Agency.
- National Reconnaissance Office.
- National Security Agency.
- Naval Criminal Investigative Service.
- Office of the Director of National Intelligence Open Source Center.

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY07

We fear the abruptness with which a lead in science and technology can be lost—and the difficulty of recovering a lead once lost, if indeed it can be regained at all.

--The National Academy of Science, 2007

Unrelenting Threat

The United States remains the prime target for foreign economic collection and industrial espionage as a result of its worldwide technological and business leadership. Indeed, strong US international competitiveness underlies the continuing drive by foreign collectors to target US information and technology.

Analyzing the extent of the threat and tracking it are becoming increasingly difficult challenges. Globalization and the growth of multinational corporations blur the lines between foreign and domestic companies, encourage outsourcing of research and development, and lead to the establishment of foreign bases of operation, all of which present more opportunities for foreign entities to target US information and technologies and mask their collection activities.

While these challenges make it increasingly difficult to measure fully the extent of industrial espionage, there was ample evidence in FY 2007 that the problem remains severe:

- The Federal Bureau of Investigation (FBI) opened 51 new cases and pursued 53 pending cases during the reporting period.
- US Immigration and Customs Enforcement (ICE) worked in excess of 2,600 export investigations. These investigations resulted in 188 criminal arrests, 178 indictments, and 127 convictions.
- The Department of Commerce's Bureau of Industry and Security (BIS) participated in excess of 783 export investigations and initiated 497. This resulted in 16 criminal convictions, $25 million in criminal fines, $1.4 million in forfeitures, 75 administrative cases, and $6 million in civil penalties.
- The Defense Security Service (DSS) received 6,034 reports of potential foreign contacts from cleared defense industry members and referred 2,879 for analysis. DSS categorized 876 as CI threats to the cleared defense industry.

Wide Ranging Group of Actors

Businessmen, scientists, engineers, and academics as well as state-run security services from a large number of countries continue to target US information and technology, according to information compiled during the FY 2007 reporting period. The bulk of the collection activity, however, comes from denizens of a core group of fewer than 10 countries, which includes China and Russia.

Europeans See Similar Threats: An Open Source Perspective

Many European countries appear to face industrial espionage threats from China, Russia, and others that are similar to threats facing the United States, according to the media. Chinese economic espionage, these sources report, focuses on industrial, scientific, and technical targets. Russian espionage specializes in military technology and gas and oil industry technical expertise. France has established a national-level government organization to counter economic espionage, while other European countries primarily leave it up to individual companies to protect against trade secret theft and enforce intellectual property rights. Targets of industrial espionage throughout Europe range from defense firms with access to military secrets to energy and drug companies.

Enduring Methods

The methods employed by collectors remain as diverse as the collectors. The methods most frequently reported by the Counterintelligence (CI) Community include:

- Requests for information.
- Solicitation and marketing of services.
- Acquisition of technology and companies.
- Official foreign visitors.
- Exploitation of joint research and contacts.
- Conferences, conventions, trade shows.
- Cyber attack and exploitation.
- Foreign collection against US travelers overseas.

Requests for Information

Direct and indirect requests for information continue to top the list of methods most often reported by the CI community. These types of approaches often include requests for classified, sensitive, or export-controlled information that are not sought or encouraged by the target. Defense Security Service (DSS), Air Force Office of Special Investigations (AFOSI), and Army Counterintelligence Center (ACIC) all report that this technique is the method of choice for both government and non-government collectors.

- ACIC numbers indicate that over 85 percent of targeting incidents involved direct requests in person or via e-mail, telephone, or fax.
- DSS reporting shows that 26 percent of its targeting incidents fall under this category.

Solicitation or Marketing of Services

Foreign companies also seek entrée to US firms by pursuing business relationships that enable them to gain access to sensitive or classified information, technologies, or projects. For example, foreign businessmen submit unsolicited business proposals offering a variety of services such as product design, software, or engineering to US military facilities conducting work involving sensitive technologies.

Acquisition of Technology

The direct and indirect acquisition of technology and information via third countries, the use of front companies, and the direct purchase of US firms or technologies are proven methods of acquisition that collectors continue to exploit, according to FY 2007 data. Countries with close ties to the United States that are subject to few US export restrictions often serve as prime locations for companies wishing to divert sensitive US technologies. Foreign collectors further disguise their activity by passing US technologies through fictitious companies, multiple layers of freight forwarders, multiple countries, or Free Trade Zones. They also commingle illicit and legal trade to obscure their activity.

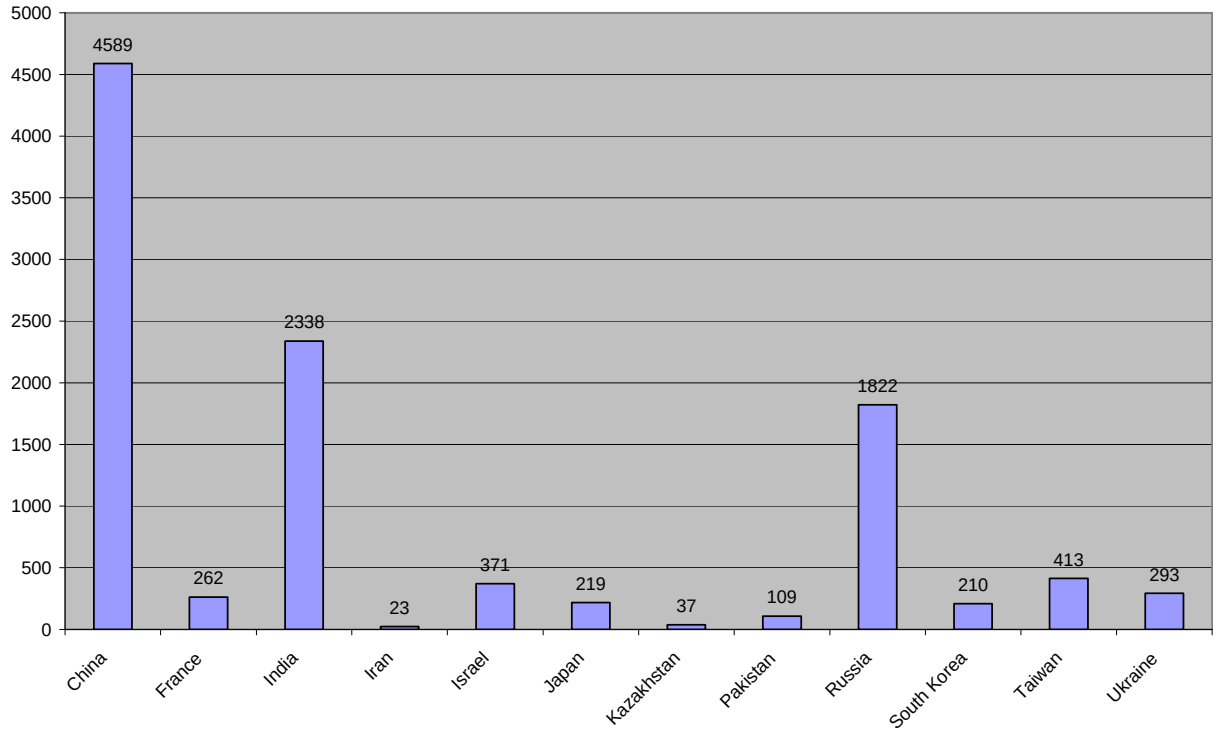
Conferences, Conventions, and Trade Shows

These public venues are laden with opportunities for foreign collectors to interact with US experts and glean information regarding dual-use and sensitive technologies. DSS notes that collection in these open

forums accounted for over four percent of reported suspicious incidents in FY 2007.

Other large scale international events, particularly athletic events, have also emerged as venues for increased economic espionage against the United States. US corporations often sponsor such events and send thousands of employees to the festivities. This year's Summer Olympic Games in China, the 2010 World's Expo in Shanghai, and the 2014 Winter Olympics in Sochi, Russia will all take place in high-threat environments. Such events offer host-country intelligence agencies the opportunity to spot, assess, and even recruit new intelligence sources within the US private sector and to gain electronic access to companies' virtual networks and databases through technology brought to the events by corporate personnel.

Number of Foreign Visitors to DOE Facilities, FY07



Official Foreign Visitors

Foreign government organizations, including intelligence and security services, also frequently target and collect information through official contacts and visits to the United States. These include visits to US military posts, armament-producing centers, and national laboratories.

Exploitation of Joint Research

Increasingly, frontier research and development is the product of cooperative efforts between US and foreign experts. As noted in a recently released Department of Commerce-sponsored study, "Individual United States firms, along with their international competitors, are building global research enterprises. American universities are establishing campuses abroad, creating joint educational programs with foreign institutions, and partnering with foreign faculty in the conduct of cutting-edge research". DOE reports that scientific exchange is integral to research across the complex of its component laboratories. Although most government organizations and private-

sector firms employ mitigation strategies to protect against illegal technology transfers and loss of trade secrets, the volume of joint research underway presents a prime targeting opportunity, either through human-to-human contact or via technical means. In FY 2007 alone, there were over 10,000 foreign visitors to DOE facilities, of which over 4,500 were Chinese. (*See chart above*)

Cyber Attack and Exploitation

Cyber threats continued unabated in FY 2007, according to a variety of reporting. The FBI opened 48 new cyber-related cases and closed four in FY 2007. Throughout the year, both US Government and cleared defense contractor networks experienced intrusions that appeared designed for intelligence collection purposes.

- Since 2002, the United States has identified China-connected computer network intrusions that have compromised thousands of hosts and hundreds of thousands of user accounts and exfiltrated terabytes of data from US, allied, and foreign government, military, and private-sector computer networks.

- Actors conducting a subset of intrusion activity affiliated with China have used socially engineered e-mails to compromise the computers of cleared defense contractors.

US Government networks are being continuously probed and targeted by both state and non-state actors for a wide variety of reasons, including legitimate cooperative scientific research. Chinese networks are the source of a significant amount of malicious activity targeting computers in the United States, but it is often difficult to attribute the origin or specific intent of any given activity. Many countries and criminals are able to get into the PRC's networks and use its Internet protocols (IP) to obscure the origin of their attacks against other targets.

"Spear phishing" is a burgeoning social engineering-based method used by hackers to gain access to sensitive information. In contrast to the broader phishing schemes—known as "spamming"—spear phishers target their attacks on fewer individuals of higher value by using open source information to develop e-mail messages that appear to originate from a trusted source and that contain enough valid information to entice the victim to open a malicious attachment or access a malicious website, according to a Microsoft alert.

In February 2007, several high ranking business executives received a spear phishing e-mail allegedly from the US Better Business Bureau. The e-mail claimed that complaints had been filed against the executives' companies and directed them to download the complaint by accessing the listed website, according to a computer forensics expert. Once downloaded, the site was designed to install a key logger on the victims' systems in order to capture all key strokes related to financial and government websites visited by the victims, according to the same source.

Foreign Targeting of US Travelers Overseas

Foreign collectors also target US travelers—businessmen, US government employees, and contractors—overseas. Collection methods include everything from eliciting information during seemingly innocuous conversations to eavesdropping on 'private' telephone conversations to downloading information from laptops or other digital storage devices after surreptitiously entering hotel rooms.

BOX: Case Study: A Chinese Collector

While most of those convicted in FY 2007 of stealing US technologies or trade secrets for transfer abroad came from the private sector. With no apparent links to foreign security services, foreign government collectors remained active as well. For example, the 2007 conviction of a Chinese-American agent who operated in the United States for more than 20 years illustrates the elusive collection threat the United States faces from foreign intelligence services.

The agent, a Chinese engineer, entered the United States via Hong Kong in 1978 and began a steady rise to positions with increasing access to sensitive information, including a position with a major US intelligence and defense contractor. In interviews with the FBI after his arrest, the agent admitted that he had passed information on sensitive projects to China beginning in 1983. By 1985 he and his wife became naturalized US citizens, and in 1996 he was granted a secret security clearance. He continued espionage activities on behalf of China, traveling there with his wife approximately once every two years to deliver information to his handler in the People's Liberation Army (PLA) and receive additional tasking.

In May 2001, the Chinese agent's younger brother, a former PLA propaganda officer, his wife, and their son immigrated to the United States. They became Permanent Resident Aliens, while working as couriers for the PLA. The agent uploaded sensitive US defense information to removable media and passed it to his brother. The brother and his wife traveled to China, often flying from Vancouver to Hong Kong in an effort to obscure their final destination. Their adult son also traveled to China, where he met with the PLA officer and received tasking that, upon his return to the United States, he passed to the agent.

The case offers insights into clandestine operational methods employed by the Chinese Intelligence Services to obscure their activities. For example, for communications security, the Agent and family members avoided phone calls from the United States to China. They also avoided direct flights. In addition, they encrypted information on laptops and disks and employed code words. Most importantly, the case demonstrates the PRC's patient and purposeful approach to espionage. The agent was allowed time to slowly infiltrate a company until he was in a position to provide sensitive information.

The case also showed the range of information and technologies that China may task a single, well-connected asset to collect against. Tasking documents recovered by the FBI included instructions to "join more [professional] organizations and participate in more seminars with special subject matters and then compile the special conference material on a disk." Also included was a list of military technologies that the agent should target, including space application, propulsion technology, nuclear attack technology, and a host of other sensitive technologies.

Targeted Information and Sectors

Foreign collectors continue to seek a wide range of unclassified and classified information and technologies.

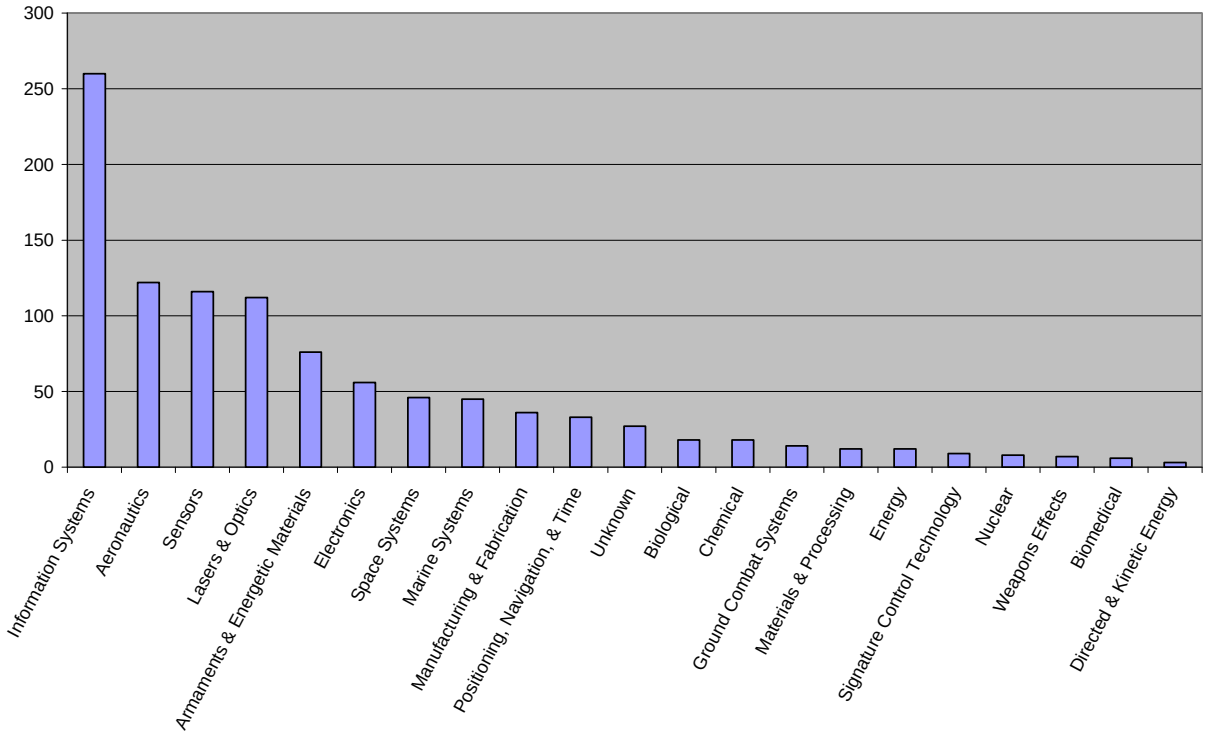
- DSS found in FY 2007 that foreign collectors attempted to obtain information and technologies from each of the 20 categories on the Developing Sciences and Technologies List. The DSTL is a compendium of scientific and technological capabilities being developed worldwide that have the potential to significantly enhance or degrade US military capabilities in the future. Of particular interest were information systems, aeronautics, sensors, and lasers and optics, according to information amassed by the DSS. *(see chart below)*

- In the same year, ACIC found that aeronautics systems, sensor technology, manufacturing and fabrication technology, and energy and power systems technology were the most frequently targeted by foreign entities. *(see chart below)*

- AFOSI highlighted aeronautics systems, manufacturing and fabrication, and information technology systems technologies as the most often targeted sectors and technologies.

- The most heavily targeted sectors across all agencies include aeronautics, information technologies, lasers, sensors, and armaments and energetic materials.

US Defense Technologies Targeted in FY07, Defense Security Service



Appendix A:

CI Community Efforts to Protect Technology

The United States CI Community encompasses a broad set of Federal agencies and departments, each of which works to protect sensitive information and technologies from unlawful foreign acquisition. The CI community includes intelligence collectors, analysts, and law enforcers, who meet regularly in a variety of forums to ensure the timely sharing of information and rapid prosecution of key cases. A sample of the support provided by Community members includes:

- **The Office of the National Counterintelligence Executive (ONCIX)** spearheads a number of efforts—including this assessment—that provide impetus to, and an organizational hub for, the Community to combine resources to track CI threats to the nation. The CI Community also supports the ONCIX Community Acquisition Risk Section (CARS), which evaluates the risk to the IC posed by US commercial entities that conduct business with foreign firms. CARS, with CI Community support, also provides threat assessments to the Committee on Foreign Investment in the United States (CFIUS) to help ensure that foreign investment does not endanger US strategic interests.

- The **Air Force Office of Special Investigations' (AFOSI's)** Research and Technology Protection's (RTP) program identifies critical Air Force technologies, analyzes threats against those technologies, directs measures to mitigate those threats, and investigates suspicious activities by foreign nationals when warranted. AFOSI also shares RTP-related intelligence with other US Government agencies and cooperatively tracks and analyzes the changing nature of the threat to American technologies.

- The **Army Counterintelligence Center (ACIC)** supports the Department of Defense in characterizing and assessing the efforts of foreign entities—government and private—to unlawfully target or acquire critical US technologies, trade secrets, and proprietary technology information. ACIC produces assessments for technology programs based on data resident in the SENTINEL CI database and assesses a foreign country's ability and willingness to protect US technology from unauthorized transfer or disclosure.

- The **Defense Intelligence Agency (DIA)** assesses foreign intelligence efforts to obtain classified and critical US technologies. DIA examines the means used to collect against US targets, including those by foreign intelligence and security services, and the impact of theft. In addition, DIA supports DoD acquisitions by working with CARS to protect against foreign intelligence collection. DIA also helps protect critical DoD technologies through its participation in the Intelligence Community process to examine foreign ownership, control, and/or influence of US assets and provide input to CFIUS.

- The **Department of Energy (DOE)** facilities and National Laboratories employ a variety of CI countermeasures to protect against the loss of critical nuclear technologies. The DOE Office of Intelligence and Counterintelligence oversees a number of programs aimed at countering the threat from foreign acquisition. Programs include policy development, field oversight, professional training, awareness training, analysis of CI threats, and investigations and operations support. DOE CI personnel have limited investigative authority to support the Federal Bureau of Investigation in the conduct of CI investigations and offensive CI operations. Since the close of the reporting period for this FY 2007 annual update, Congress approved the reintegration of DOE and Nuclear Security Administration CI programs, which cleared the way for complete consolidation of all intelligence-related activities at the Department of Energy.

- The **Defense Security Service (DSS)** implements the National Industrial Security Program at approximately 12,000 cleared defense contractor facilities across the United States. In FY 2007, DSS CI specialists provided 524 threat awareness briefings to more than 19,163 cleared defense contractor employees. They also made 8,743 referrals of suspicious incidents to investigative

agencies, resulting in 868 investigations. DSS also produced 899 intelligence information reports for dissemination throughout the CI Community. On the basis of suspicious incidents reported by contractors, DSS CI traced and analyzed the changing nature of the threat to US technologies. CI specialists teamed with DSS Industrial Security Specialists on nearly 191 security reviews of contractor facilities, using current threat information to assist contractors in developing tailored security countermeasures.

- The **Federal Bureau of Investigation's (FBI's)** Counterintelligence Division is responsible for most of the Bureau's efforts to prosecute and prevent economic espionage in the United States. The division relays the seriousness of foreign threats to US companies, laboratories, and other US entities by providing presentations, publishing tactical and strategic intelligence products, and hosting meetings and working group sessions. Within the Counterintelligence Division, the Counterespionage Section handles investigations that fall under the purview of the Economic Espionage Act of 1996. This section administratively supports and gives operational assistance to FBI field divisions that undertake these investigations. The Counterintelligence Division's Domain Section, which began operations in August 2005, oversees efforts to identify and address CI vulnerabilities and threats to critical technologies. The section maintains national security-related liaison initiatives through business and academic alliance programs and provides strategic CI operational leadership and focus through national and regional working groups.

- The **National Geospatial-Intelligence Agency's** (NGA's) Office of Counterintelligence works to protect the agency's capabilities, personnel, and facilities. NGA is building the Threat Mitigation Center, which is designed to further integrate and enhance NGA collaborative efforts in areas such as operational security, industrial security, and information assurance. To achieve synergy between the CI and law enforcement communities, NGA has established a full-time presence at the ONCIX CARS. NGA also created a Research Technology Protection Oversight Council to design, develop, implement, and evaluate tactics, techniques, and procedures required to protect new technologies through all stages of the acquisition, research, development, test, and evaluation process.

- The **National Reconnaissance Office (NRO)** has worked to improve the identification of espionage threats to its operations, programs, and personnel as well as increase the awareness of targeting efforts by nontraditional threat countries and groups. In support of its contractor community, CID provides tailored briefings of current threats to technology and targeting methods. In addition, CID's CINet system is a secure, automated, Web-based intranet system that uses electronic forms to streamline the reporting of foreign contact and foreign travel, allowing for the dissemination of threat information and briefings to security officers and authorized users within, and outside of, government facilities. The CINet further provides users with a means of submitting requests for specific CI services. CID is working closely with the FBI's Domain Task Force and other mission partners to protect NRO resources and enhance the RTP program. It has also placed a CI representative at CARS to support NRO requirements and the overall CARS mission.

- The **DNI Open Source Center (OSC)** contributes to the CI Community's effort against China by monitoring foreign-language publications and Internet web sites for indications of threats, sharing this information with appropriate agencies, including law enforcement. OSC translates significant open-source materials on CI issues. It monitors European media reporting on economic intelligence and industrial espionage. OSC has taken the initiative in organizing Community conferences and working groups aimed at countering specific CI challenges and has supported a wide variety of *ad hoc* requests from offices throughout the Intelligence Community.

Appendix B**: Selected Arrests and Convictions for Economic Collection and Industrial Espionage Cases in FY 2007**

Country	Technology	Status	Source
China	Restricted Night Vision Data	US firm pled guilty to illegally exporting restricted night vision data and omitting statement of material fact in required arms export reports	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007
China	Conspiracy to export current and future US Navy warship technical data	Naturalized US citizen and Navy contractor found guilty at trial, May 2007; wife charged with acting as an unregistered agent of the PRC, June 2007	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007
China	Illegal export of military source code to China's Navy Research Center	Canadian citizen of Chinese origin pled guilty to violating the Economic Espionage Act (EEA), August 2007	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007; USA Today, December 14, 2006
China	Controlled microwave circuits	US citizen pled guilty to illegal export without required DOC authorization, August 2007	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007
China	Controlled microwave amplifiers with potential radar applications	US firm and US citizen settled charges of 44 violations of the EEA for knowingly exporting unlicensed item and filing false declarations	DOC Bureau of Industry and Security (BIS) Export Enforcement, Major Cases List, February 2008

Country	Technology	Status	Source
China	Trade Secret theft	US citizen and Chinese national charged with economic espionage and trade secret theft, September 2007	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007; PC World, September 28, 2007
Cuba	Controlled telecommunications equipment (national security, anti-terrorism, and encryption)	US firm pled guilty, April 2007	BIS Export Enforcement, Major Cases List, February 2008
India	Illegal export of space launch vehicle and ballistic missile-related information	Singaporean passport holder of Indian heritage and US permanent resident of Indian origin arraigned on charges of illegal export, April 2007	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007; the Indian Express, April 1, 2007
India	Vibration amplifiers, cable assemblies, and vibration processor units	US firm manager charged with illegal export to an Indian facility designated by US as an end-user of proliferation concern, July 2007	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007
Indonesia	Scheming to purchase and illegally export more than $1 million worth of machine guns, sniper rifles, and other weapons to Indonesia, the defendant also made inquiries about purchasing Sidewinder missiles and strafing ammunition for illegal export to Indonesia	Indonesian national pled guilty to conspiracy to violate the Arms Control Export Act and money laundering, January 2007	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007, Honolulu Star Bulletin, January 19, 2007

Country	Technology	Status	Source
Iran	Illegal export of 3 KeyMaster Software	Naturalized US citizen, former nuclear plant engineer, of Iranian heritage arrested and charged with illegal export, April 2008	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007; the Arizona Republic, April 21, 2007
Iran	US military aircraft parts/maintenance kits for the F-14 fighter jet	US citizen sentenced for violation of International Emergency Economic Powers Act, May 2007	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007; the Orange County Register, May 9, 2007
Iran	Illegal export of laboratory equipment	US person pled guilty to conspiracy for attempting to export two lab equipment systems to Iran, July 2007	BIS Export Enforcement, Major Cases List, February 2008
Iran	Illegal export of F-14 components	Pakistani citizen arrested on charges of illegal export to Malaysia for probable use by Iran, July 2007	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007; Associated Press, July 19, 2007
Iran	Illegal export of aircraft parts to Iran	CEO of US firm sentenced to five years probation and fines, July 2007	BIS Export Enforcement, Major Cases List, February 2008

Country	Technology	Status	Source
Iran	Attempted illegal export of night vision goggles, and submachine guns	Iranian-born American citizen entered guilty plea, August 2007	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007; Associated Press, August 30, 2007
Iran	Illegal export of Aerospace grade aluminum, aircraft, components, and other equipment	Netherlands-based aviation services company, its Dutch owner, and two other Dutch companies charged September 2008	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007
Iran	F-4 and F-14 components	Two US citizens charged with attempted illegal export of restricted components to Canada for probable use by Iran	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007
Iran	16 export shipments of equipment described as "gaskets, ball bearings, auto parts, oil, or fuel filters and other parts and accessories for tractors"	US firm president sentenced for aiding and abetting operation of unlicensed money transmitting business, October 2007	BIS Export Enforcement, Major Cases List, February 2008
Iran	Pipe cutting machines	October 2007, a Swiss national, an Iranian national, and a US company sentenced after pleading guilty on August 20 to one count of making false statements for involvement with the attempted export of pipe cutting machines to Iran via Germany	BIS Export Enforcement, Major Cases List, February 2008

Country	Technology	Status	Source
Iran	Illegal export of nickel alloyed pipes to Iran via UK and UAE	November 2007, a British corporation pled guilty in US District Court to one count of violating the International Emergency Economic Powers Act for an attempted export without an export license	BIS Export Enforcement, Major Cases List, February 2008
Iran	US origin valves	US citizen sentenced for aiding and abetting a conspiracy to export valves to Iran via Australia	BIS Export Enforcement, Major Cases List, February 2008
Iraq	Telecommunications equipment/technology	Naturalized US citizen of Chinese origin pled guilty to making false statement to the FBI and operating as a representative for the technology procurement arm of the Chinese government, April 2007	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007; US Department of Justice News Release, May 1, 2006
Iraq	Telecommunications and other equipment	Two US persons indicted on charges of violating the International Emergency Economic Powers Act, money laundering conspiracy, and false statements, July 2007	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007
Pakistan	Restricted graphite products with nuclear and missile applications	US firm sentenced for conspiring to falsify documents and make false statements about a 2003 illegal export to the United Arab Emirates that ultimately ended up in Pakistan, October 2007	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007

Country	Technology	Status	Source
Suriname	Controlled ballistic missile helmets	US firm pled guilty to unlicensed export activity and making false statements on an export declaration, March 2007	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Year, October 11, 2007
Taiwan	Controlled nickel powder	One person pled guilty to one count of making false statements related to illegal export of nickel powder, October 2007	BIS Export Enforcement, Major Cases List, February 2008
United Arab Emirates	Controlled graphite	US firm president and representative pled guilty to conspiracy to commit several federal violations, misleading federal investigators, and falsification of documents related to shipment of graphite products	BIS Export Enforcement, Major Cases List, February 2008


OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA


NATIONAL COUNTERINTELLIGENCE EXECUTIVE
UNITED STATES OF AMERICA